In the Specification

Please replace the paragraph beginning at page 5, line 31, with the following:

A1

--The problems with systems like that shown in Fig. 1 are keenly felt in many computer and communication systems, including as just one example those employed in electronic commerce. As paper documents that have traditionally recorded transactions, such as the purchase of an object, the withdrawal of bank funds, or the execution of a contract, are replaced by electronic records, serious issues of physical control of the electronic records and access to them are raised. Systems and methods for providing a verifiable chain of evidence and security for the transfer and retrieval of electronic records and other information objects in digital formats have been described in U.S. Patents No. 5,615,268; No. 5,748,738; and No. **6,237,096**; all to Bisbee et al., and U.S. Patent Applications No. 09/452,928, filed on December 2, 1999, and No. 09/737,325, filed on December 14, 2000, both by Bisbee et al. These patents and applications are expressly incorporated here by reference, and describe among other things flexible business rules that enable users to have roles that are required or enabled only at particular points in a transaction or process. For example, a user may have a role of title agent only after a transaction has closed.--

Please replace the paragraph beginning at page 19, line 7, with the following:

A2
N.W.

--The Request Counter field is typically initialized at zero at the creation of the Security Context and is incremented each time a User Request with this particular Security Context is directed to the Stateless System Components 535. In this way, use of the Security Context can be limited, with the User being denied access should the Request Counter exceed a predetermined maximum. It will be appreciated that decrementing Request Counters can also be used. Additionally, the Request Counter may be used to match Requests with System Component responses when responses are returned asynchronously (out of chronological order). Thus, a request counter is included in the request for access, and **[If]** if access is granted, a response is sent to the user that includes the a request counter, which the user uses to match the response, which may be an acknowledgement of an action performed (e.g., creation of a "certified"

A2

N.E.

printout of a record), to the request. Finally, the Request Counter can prevent "replay" attacks, in which a hacker intercepts a User Request or Component Response and falsely presents the Request for access to a protected transaction or record or replays the Response to create network and system congestion. The system 530 and client application 520 both recognize when the Request Counter in the Security Context/User Request data stream is out of synchronization with previous Requests and reject the false Request. Alternatively, Client Time (Fig. 6b) can also be used to prevent replay attacks.--